Technischer Überblick

Projekt "Schulen ans Internet" (SAI)

INHALT

Swisscom (Schweiz) AG
Grosskunden
Postfach
3050 Bern

1. Zweck

Swisscom (Schweiz) AG offeriert den Kantonen zu einmaligen Konditionen ein Bildungsnetz, das alle LANs (lokale Netzwerke) der Schulen zu einer einzigen Kommunikationsinfrastruktur mit garantierten Bandbreiten/Antwortzeiten untereinander verbindet und einen zentralen Internetanschluss mit grosszügiger Bandbreite bietet.

Ist eine Schule erst einmal am Netz, können Schülerinnen und Schüler sowie Lehrkräfte unbeschränkt ohne Volumenbegrenzung und kostenlos rund um die Uhr das Internet nutzen. Für die Sicherheit sorgt eine zentrale Firewall, die das Bildungsnetz gegen unberechtigte An- und Zugriffe von und nach aussen schützt.

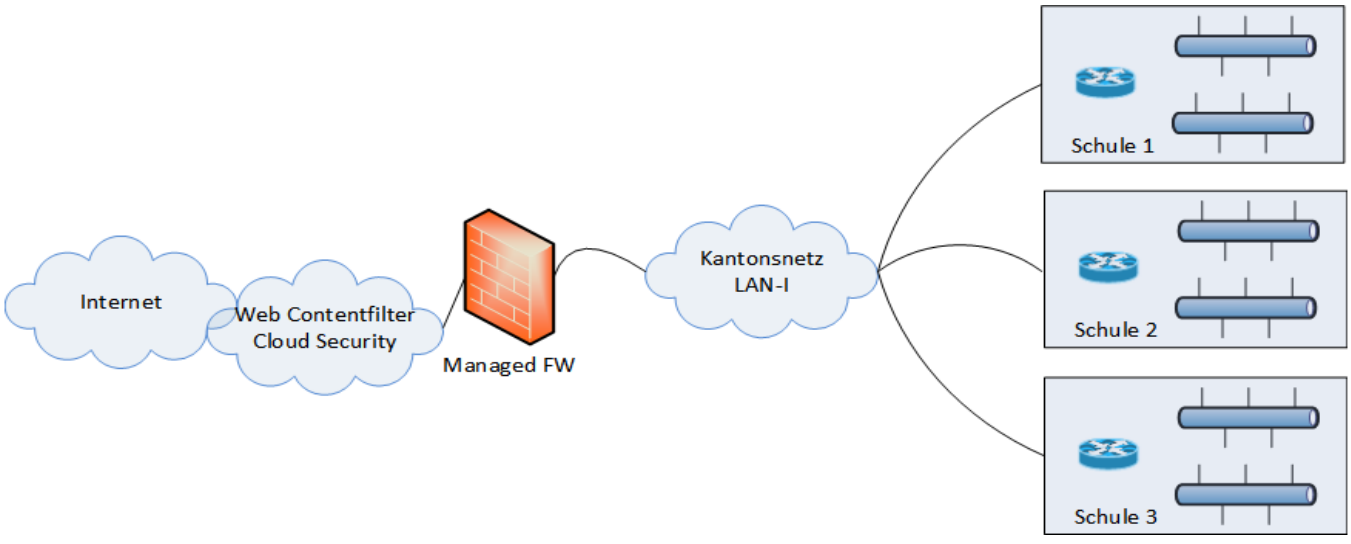
Diese Richtlinie zeigt die technischen und organisatorischen Rahmenbedingungen für den Anschluss der Schulen innerhalb des Kantons auf.

Angebot Standard
> SecurePop Managed Firewall, die unberechtigte Zugriffe von aussen abwehrt.
> Cloud Securtiy Service, Inhaltsfilter, der den Zugriff auf ungeeigneten Inhalt im Internet verhindert.

Angebot Extra und Spezial
> VDSL Business Access entry (bis 30/10 MBit/s)
> Glasfaser Office Access (bis zu 50/10 MBits/s)
> Business Enterprise-Access (ab 2/2 MBit/s bis 200/200 MBit/s)

Für die Anschlüsse mit höherer Bandbreite **Extra** und **Spezial** entscheidet der Kanton, wer die Sicherheitslösung zur Verfügung stellt.

1.1 Contentfilter



2. Grundsätze

Das Bildungsnetz für den Anschluss der Schulen ans Internet wird völlig **getrennt** von den administrativen Netzen der einzelnen Kantone aufgebaut. Kommunikationsbeziehungen zu internen kantonalen Stellen (nicht Schulen) sowie zu den anderen kantonalen Bildungsnetzen erfolgen ausschliesslich über die zentrale Internet **Firewall** des kantonalen Bildungsnetzes (pro kantonales Bildungsnetz eine Firewall).

Für die einzelnen Bildungsnetze betreibt Swisscom AG ein **Helpdesk.**
Störungen können ausschliesslich via die kantonale Koordinationsstelle Swisscom AG gemeldet werden. Die Schulen sind verpflichtet, sich bei allfälligen Störungen an die kantonale Koordinationsstelle zu wenden.

Die **Installationskosten** durch konzessionierte Elektriker für schulinterne Verkabelungen für den Anschluss ans Bildungsnetz werden durch die Schulen (resp. die Kantone) übernommen. Die Schulen sorgen in ihren Gebäuden für geeignete räumliche und klimatische Bedingungen (MODEM, Router).

3. Zusammenfassung der Lösung

Das von Swisscom AG implementierte und betriebene Netzwerk basiert auf dem LAN-I-Service sowie dem Managed Firewall *expert* Service der Swisscom AG.

Die Schulen erschliessen ihre Endgeräte (PC, Drucker) über ein Ethernet LAN und schliessen dieses an den Swisscom AG eigenen CISCO-Router vor Ort an. Alle Router stellen untereinander pro Kanton ein geschlossenes Layer-3-Netzwerk mit any-to-any-Konnektivität dar, welches einen einzigen zentralen und gesicherten Übergang zum Internet besitzt. Für den Schutz wird eine Firewall (Managed Firewall *expert*) eingesetzt, deren Regelwerk ("Policy") für alle angeschlossenen Schulen gilt.

Optional steht ein Web Content Screening zur Verfügung. Pro Kantonsnetz kann definiert werden, welche verfügbaren Kategorien erlaubt oder geblockt werden. Über eine begrenzte Anzahl an Black- resp. Whitelist-Einträgen können die Filter für spezifische Bedürfnisse angepasst werden.

4. IP-Adressierung

Swisscom AG erstellt das **IP-Adressierungskonzept** , damit erhält jede Schule einen eindeutigen IP-**Adressbereich.**
Bestehende interne IP Adressierungen müssen auf Grund der neuen Adressierung durch die Schulen **umgestellt** werden.

Die **Endgeräte** der Schulen müssen entweder fix oder via schuleigenes DHCP adressiert werden. Die DHCP- Funktionalität ist nicht Bestandteil der Swisscom-Lösung. Dazu ist der pro Schule zugeteilte Adressbereich zu verwenden. Die ersten fünf IP-Adressen (pro Subnetz) sind für Swisscom AG reserviert und dürfen nicht belegt werden.

5. Security Policy

Die Policy an der zentralen Firewall des jeweiligen kantonalen Bildungsnetzes gilt **für alle** angeschlossenen Schulen.

Die implementierte Policy ist auf Wunsch der Bildungsverantwortlichen **offen** definiert und entspricht nicht den üblichen restriktiven Securitypolicies für Firewalls im Geschäftskundenbereich. Dadurch können erhöhte Sicherheitsrisiken entstehen. Auf der zentralen Firewall erfolgt weder Benutzerauthentifizierung noch Virenscanning.

6. Inhouse LAN-Vernetzung

Das LAN und dadurch vernetzte Peripheriegeräte (PC, Drucker) werden mit privaten IP-Adressen gemäss
Adressierungskonzept von Swisscom AG adressiert. Allfällige Hilfsmittel für die Administration der Netzwerke wie DNS Server oder DHCP Server müssen durch die Schulen/Kantone beschafft und betrieben werden.

Schulen und insbesondere Kindergärten, die keinen eigenen Telefonanschluss besitzen, und allenfalls an einer Telefonvermittlungs-Anlage (PBX) angeschlossen sind, benötigen für den Internet-Anschluss durch *Schulen ans Internet“ keinen zusätzlichen Telefon-Anschluss.

7. Organisation und Betrieb

Pro Kanton ist eine **zentrale Koordinationsstelle** für das kantonale Bildungsnetz bezeichnet. Deren Aufgaben gegenüber Swisscom AG und den angeschlossenen Schulen umfassen:

- Die Bearbeitung und Weiterleitung der Anträge der kantonalen Schulen.
- Die Bearbeitung von Konfigurationsänderungen an der zentralen Firewall zu Handen Swisscom AG.
- **Alleiniger Ansprechpartner** für die Schulen bei technischen oder betrieblichen Störungen im kantonalen Bildungsnetz.
- **Einzige** kantonale Schnittstelle zum dedizierten SAI-Helpdesk bei Swisscom AG.

Pro Schule ist ein **technischer Ansprechpartner** zu bezeichnen. Störungen im kantonalen Bildungsnetz werden durch die technischen Ansprechpartner an die kantonalen Koordinationsstellen gemeldet.

8. Technische Informationen

8.1 Mailboxen bei ISP gehostet

Normalerweise lassen Mail-Provider das Versenden von Emails über ihre Server nur aus dem eigenen IP-Adressbereich zu. Um aus den SAI-Netzen trotzdem Mails aus externen Mail Accounts versenden zu können, stehen zwei Möglichkeiten zur Verfügung:

8.2 SMTP-Authentisierung

Die meisten Mail-Provider bieten heute SMTP-Authentisierung an. Dies ist die einfachste Methode zum Versenden von Mails über einen externen SMPT-Server.

8.3 IP-Plus Mail Relay

Die Schule konfiguriert auf den Clients den IP-Plus-Mailserver mailout.ip-plus.net als SMTP-Server zum Versenden von Mails (anstelle von z.B. mail.bluewin.ch). Dieser Server wurde speziell für "Schulen ans Internet" bereitgestellt und ersetzt die beiden früher angegebenen Server:

- mailhost.ip-plus.net
- smtp.ip-plus.net

Falls bei Schulen einer dieser Server noch benutzt wird, sollte ein möglichst baldiger Wechsel auf den neuen Server in Betracht gezogen werden.

9. DNS-Server

Sofern die Schule nicht einen eigenen DNS-Server betreibt, kann sie auf den Clients und Servern die folgenden beiden IP-Plus DNS-Server eintragen:

sdns1.ip-plus.net 164.128.36.36
sdns2.ip-plus.net 164.128.36.37

Die Standard-DNS-Server von IP-Plus stehen für SAI nicht zur Verfügung.

10. Privater IP-Adressbereich (Zone INTRANET)

Das Swisscom IP-Adresskonzept sieht für die Adressierung von Computern in der Schule Adressen aus dem privaten Bereich 10.x.x.x vor. Die pro Kanton zentrale SecurePoP-Firewall erlaubt für diesen Adressbereich alle gängigen Services, die ein PC benötigt (http, ftp, pop3, smtp etc.). Auf Wunsch werden spezifische Ports von der Zone INTRANET ins Internet geöffnet. Die Portöffnungen betreffen immer das gesamte Kantonsnetz und kann nicht auf einzelne Schulen oder IP-Adressen eingeschränkt werden.

Das Erreichen eines Servers im 10.x.x.xer Adressbereich aus dem Internet wird nicht unterstützt. Diese Adressen werden vom Internet her hinter der öffentlichen Adresse der Firewall (212.x.x.x) durch Network Address Translation (NAT) versteckt.

11. Öffentlicher IP-Adressbereich (Zone Public_Servers)

Für Systeme, die vom Internet her direkt adressierbar sein müssen (sog. „Public_Servers“) wird eine beschränkte Anzahl öffentlicher IP-Adressen zur Verfügung gestellt. Die pro Kanton zentrale SecurePoP-Firewall erlaubt für diesen Adressbereich alle gängigen Services. Auf Wunsch werden spezifische Port zwischen der Zone „Public_Servers“ und dem Internet in beiden Richtungen geöffnet. Die Portöffnungen betreffen immer das gesamte Kantonsnetz und kann nicht auf einzelne Schulen oder IP-Adressen eingeschränkt werden.

Anmerkung: Der Adressbereich für die Zone Public_Servers ist auf demselben Anschluss konfiguriert wie die Zone INTRANET (sog. Multi-Netting). Es handelt sich somit nicht um eine DMZ auf einem dedizierten Firewall Interface.

12. Schuleigene Firewall

Swisscom betreibt innerhalb der Schulinitiative pro Kantonsnetz eine dedizierte Firewall. Schuleigene Firewalls werden nicht unterstützt (ausgenommen OpenNet). Benutzt eine Schule eine eigene Firewall oder Proxy Gateway, kann Swisscom für die daraus resultierenden Serviceunterbrüche oder Performance-einbussen keine Unterstützung leisten.

13. Cloud Web Security

14. Eigenschaften des Cloud Web Security Service

- Für jedes Kantonsnetz wird ein eigener Content Filter betrieben. Individualisierung ist daher nicht für einzelne Schulen möglich.
- Filterung von Webinhalten aus 30 Haupt- und 120 Unterkategorien, sowie eigene White- und Blacklists.
- Schutz vor gefährlichen Inhalten wie Viren, Malware, Phishing und Spear Sites, mit realtime aktualisierter Datenbank
- Aktivieren der SafeSearch Funktion für Suchanfragen. Moderne Suchmaschienen und Webserver verwenden SSL . Dieser Traffic n^muss nun mir SLL Inspection analysiert.
- Die zu sperrenden Kategorien können durch die Kantonale Koordinationsstelle KKS via www.portal.securepop.ch ausgewählt werden.
- Es besteht die Möglichkeit, die Kategorie-Zugehörigkeit einer bestimmten URL abzufragen und eine neue Kategorisierung zu verlangen

14.1 Filtering von SSL verschlüsselten Webinhalten

Grundsätzlich besteht die Möglichkeit auch SSL Verschlüsselten Verkehr zu Filtern. Dies ist notwendig um die SafeSearch Funktion bei bestimmten Suchmaschinenanbietern zu erzwingen. In diesem Fall ist die flächendeckende Installation des Zscaler Root Certificate auf den entsprechenden Endgeräten notwendig.

14.2 Anonymizers Proxy

Im Internet gibt es Server (Anonymizing Proxies), die eigens dazu da sind, einen URL Filter zu umgehen und damit den Zugang auf eigentlich gesperrte Seiten zu ermöglichen. Es besteht grundsätzlich die Möglichkeit solche anonymen Proxys zu sperren.

14.3 Re-kategorisierung von Webinhalten

Die Webfiltering Datenbank enthält laufend aktualisierte Werte für Milliarden von Webseiten Weltweit. Es ist jedoch nicht lückenlos. Es kann daher vorkommen, dass einzelne Webseiten falsch kategorisiert sind. In diesem Fall ist es möglich eine Rekategorisierung vorzunehmen. Eine Rekategorisierung kann über www.portal.securepop.ch oder direkt über http://www.zscaler.com/sitereview/

14.4 Authentisierung basierend auf IP Adressen

Für verschiedene Webangebote ist es notwendig, sich anhand der Source IP Adresse zu identifizieren. Erfolgt der Zugang zu diesem Angebot über das Webfiltering müssen dazu folgende IP Adressbereiche zur Freigabe an den entsprechenden Anbieter gemeldet werden.

195.65.152.0/24
195.65.154.0/24

Hinweis: Das gilt für den Fall, dass der Zugriff auf das Angebot effektiv über den Web Security Proxy erfolgt.

15. Cloud Web Security Services

Welche URL Kategorien sind gesperrt?
Es gibt 30 URL Filter Kategorien und etwa 120 Sub Kategorien. Dieses Server bezieht automatisch die letzten Updates für schlechte Websites.

Wie kann ich zusätzliche Kategorien sperren oder wieder erlauben lassen?
Das Sperren und Erlauben von Kategorien geschieht über das www.portal.securepop.ch portal

Wo findet man eine Beschreibung der Kategorien?
Die Kategorien sind als solches nicht im Detail beschrieben. Die dahinter liegenden URLs werden dynamisch in Real time angepasst.

In welcher Kategorie ist die betroffene Site?
Die Seite http://zulu.zscaler.com/ ist eine URL Risk Analyser seite und gibt ein Score für die gewünschten Webseiten.

Wo kann die Zuordnung von Sites zu Kategorien geändert werden?
Ein Änderung der Zuordnung sollte nicht nötig sein da dieser Service weltweite Updates von mehrteren100M täglichen Transaktionen erhält. Wenn eine fragwürdige Webseite kategorisiert werden sollte kann dies über das www.portal.securepop.ch erreicht werden.

Warum ist eine Seite erreichbar, obwohl sie eigentlich einer Kategorie angehört, die gesperrt ist?
Das Internet ist sehr dynamisch. Gerade fragwürdige Sites wechseln oft die URL oder den Domain-Namen und sind damit vorübergehend nicht korrekt kategorisiert. Auch kommen pro Woche tausende neuer Sites hinzu, die neu zu kategorisieren sind.